Clear Discarded Storage that Contained Secrets and Do Not Read Uninitialized Storage

William L. Fithen, Software Engineering Institute [vita[3]]

2005-10-03 L4 / D/P[4]

Failing to initialize storage can introduce vulnerability.

Description

When allocated, storage may not have been initialized, meaning that whatever was left in storage from its previous use is still there. If that storage might contain leftover secrets, like passwords, then accidentally disclosing that data amounts to a security leak—of information from the previous user.

When your system, in turn, deallocates storage that contains secrets, it may be leaking those secrets to the *next* user of the storage.

References

[Thompson 05]	Thompson, Herbert & Chase, Scott. *The Software Vulnerability Guide*. Charles River Media, 211-222. 2005.
[VU#412115]	Lanza, Jeffrey P. *Network device drivers reuse old frame buffer data to pad packets*. 2003. http://www.kb.cert.org/vuls/id/412115.

Carnegie Mellon Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN “AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[3] http://buildsecurityin.us-cert.gov/bsi/about_us/authors/320-BSI.html (Fithen, William L.)

[1] mailto:permission@sei.cmu.edu